Proc. IEEE International Conference on Blockchains and
Cryptocurrency (ICBC 2021)

Future Directions for Regulated Private Wallets and VASP Trust Infrastructures

Thomas Hardjono
MIT Connection Science & Engineering
Cambridge, MA 02139, USA
Email: hardjono@mit.edu

***Abstract*—A true decentralized peer-to-peer electronic cash system requires control of private keys by end-users in private wallets. This necessitates wallet systems to utilize trusted hardware to protect keys. However, trusted hardware alone is not enough. There must be a corresponding attestation infrastructure to support the verification of evidence regarding the state of the trusted hardware, the provenance and the presence of keys, and other related configurations. This permits legitimate external entities to obtain some degree of visibility into the wallet state without access to the private keys. Relying parties, such as crypto-funds insurance providers and auditors of CBDC distributors, require such visibility for risk assessment. New VASPs have the opportunity today to invest in these emerging infrastructures.**

***Index Terms*—blockchains, attestations, wallet systems, cybersecurity, cryptography**

I. Introduction

With the green light given by the US OCC (Office of the Comptroller of the Currency) in July 2020 to allow national banks to provide cryptocurrency custody services for customers [1], many *centralized crypto-exchanges* (CEX) entities now face the business challenge from banks entering the "hosted wallet" (key custodian) market [2]. Current examples of CEX entities include Binance, Coinbase, Huobi Global and Kraken [3]. Such entities are broadly referred to as *Virtual Asset Service Providers* (VASP) by regulators [4], [5].

The vision of Bitcoin [6] is that of a peer-to-peer electronic cash system that relies on a decentralized network of nodes, where end-users would control their private keys and deal with one another directly without the mediation of any third party. Thus, needless to say, the notion of a hosted wallet at a centralized CEX goes against the very heart of this vision.

II. True Decentralization and Key Protection

Fulfilling the vision of the decentralized peer-to-peer electronic cash system necessitates the decentralization of control of private keys. That is, it necessitates end-users holding and controlling their private keys in their *private wallets* (unhosted, non-custodian). In turn, the requirement of key-protection in private wallets unavoidably points to the need for *trusted hardware* to be utilized by the private wallet systems.

Currently, the market for hardware-based wallets is still nascent, with a handful of products available for end-user consumers and enterprise customers (e.g. Ledger's Nano X [7], Silo from Metaco [8]). However, low-cost cryptographic hardware has been available for consumer PC computers since the mid-2000s, in the form of the Trusted Platform Module (TPM) chip [9], [10]. The plentiful availability of the TPM chip was spurred, among others, by the US Army purchase decision in 2006 regarding TPM-enabled laptops and PC computers [11].

Although more advanced trusted hardware technologies exist today (e.g. Intel SGX [12], Arm TrustZone [13], Microsoft Pluton [14]), the humble TPM chip is already widely available in several hundred million PC computers and related devices. Applications of the TPM chip in PC computers include file encryption (e.g. Microsoft BitLocker [15]), pairing with self-encrypting disk-drives (e.g. Seagate Black Armor [16]), and for certifiying application keys [17].

III. Trusted Hardware Alone is not Enough

However, trusted hardware alone is not enough. A wallet system utilizing trusted hardware must be able to yield *attestation evidence* for components and states that are mutable and there must be *attestation endorsements* from component vendors for the roots of trust that are not capable of detecting and/or reporting unauthorized changes to itself [18], [19]. Attestations-capable hardware in wallets is only half of the equation. There needs to be a corresponding *attestation verifier* entity or service that can appraise the evidence [20] in a *neutral* and *independent* manner, as part of a broader attestation infrastructure in the trust ecosystem.

The parties seeking the *attestation results* are not only the wallet owners (e.g. as part of cybersecurity requirements), but also legitimate external entities who need to make risk assessment decisions regarding the state of keys (and the assets bound to the keys) in the trusted hardware of the wallet. These external entities (e.g. funds insurance providers) are the *relying party* to the results coming from the verifier service (see Figure 1). They seek a reasonable degree of visibility into the state of the wallet and of the private-keys, but without access to the private-keys. Among others, they need to obtain reasonable proof that (i) the private-keys bound to the virtual assets are currently located in a specific trusted hardware inside a given wallet, (ii) that the wallet device is in possession of the user (e.g. through authenticated access to the trusted hardware in the wallet), and (iii) that extracting the private-key from the trusted hardware will be time-consuming and economically too costly for the attacker who steals the wallet device. They

978-0-7381-1420-0/21/$31.00 ©2021 IEEE

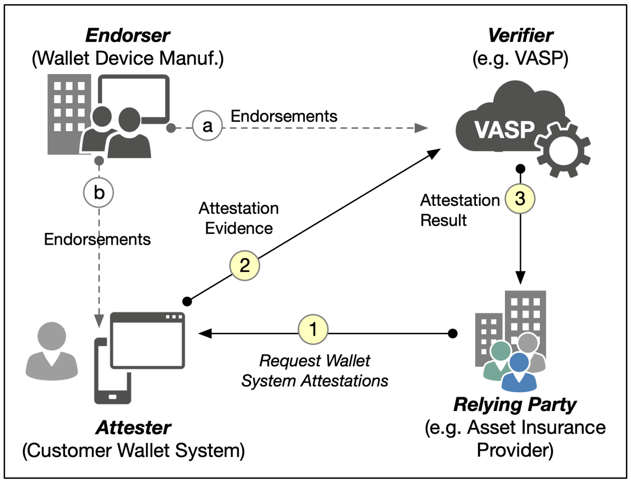

Fig. 1. Overview of wallet attestation flows (following [19], [22])

also need proof that an actual trusted hardware component is being utilized (i.e. not virtualized or software-emulated [21]).

IV. Use Cases

Two use-cases for attestations infrastructures are as follows:

- *Asset insurance providers*: An increasing number of traditional funds-insurance providers are seeking to cover for virtual assets traded on blockchain networks [23], [24]. The protection of keys are therefore a crucial factor in their risk assessment calculations. Many of them are willing to cover for keys that are placed in off-line cold storage ("cold wallets"), which is the approach taken by many CEX entities today. An attestation infrastructure that can support the appraisal of evidence from consumer "hot-wallets" utilizing trusted hardware can greatly expand the market for the entire funds insurance industry.
- *CBDC Distributors*: Several governments have indicated interest in issuing *Central Bank Digital Currencies* (CBDC) [25], [26], which may additionally permit commercial banks to issue *Stablecoins* based on baskets of CBDCs and other real-world assets [27], [28]. Although the structure of the distribution network for CBDCs currently remains undetermined, the use of blockchain technology may be attractive for groups of commercial banks wishing to circulate and distribute CBDCs and Stablecoins. Their wallet systems, blockchain gateways [29], [30], and other sensitive computer systems employing trusted hardware will benefit greatly from attestations services. External audit entities as relying parties would also benefit in seeing evidence of good key protection practices by these CBDC holders/distributors.

V. Infrastructure for Attestations

Although the subject matter of attestations (or "remote attestations") is over two decades old now [31], the concept has only recently entered the mainstream cybersecurity narrative and the components supply-chain considerations [32]. In brief, an attestation infrastructure should consists of the following functions and services [19], [22]:

- *Supply chain of endorsements*: Components manufacturers need to issue endorsements for their products [33] and to make these signed endorsements readily available to the neutral verifier services (see flow (a) in Figure 1).
- *Attestation verification providers*: An attestation verification service provider must operate in *neutral manner*, independent from the wallet manufacturers and the wallet owners. It must collect and validate the relevant endorsements from the various components manufacturers, and also verify certification evidences (e.g. FIPS certification). Its operations must be underpinned by a *legal trust framework* that allows auditing by 3rd party audit entities.
- *Attester capabilities in hardware components*: Certain types of components in trusted computing need to possess the *attester* capability. Currently, efforts are underway in the semiconductor industry to begin addressing this need more broadly (see [32], [34]).

VI. Relevant Evidence from Wallet Systems

Depending on the trusted hardware, there are a number of useful attestation evidences for various use-cases [19], [33]:

- *Evidence of wallet system configurations*: The evidence yielded by a wallet attester should include a manifest of all the hardware, firmware and software comprising the wallet system, including the version information.
- *Key creation provenance*: Most current generation cryptoprocessors and trusted hardware possess the capability to generate new private-public keys inside the shielded location of the hardware. Evidence that a key pair was *generated on-board* and evidence that the private key is *non-migrateable* contributes to the risk profile of the wallet system as a whole.
- *Evidence of geolocation of wallet*: The trusted hardware in a wallet may be utilized to retain (cryptographically seal) geolocation information generated by the GPS chip inside a mobile wallet system (e.g. smart phone) [35].
- *Key usage sequence*: Certain types of trusted hardware may permit a log of the sequence of usage of a private-key (e.g. for digital signatures) to be maintained locally. This truthful log of key usage may be verifiable by an attestation service provider for relying parties seeking to audit the wallet against the on-ledger transactions history. This type of audit history is useful for Travel Rule compliance [4], [5] and taxation regulations [36].

VII. Conclusion: VASPs as Attestation Verifiers

In the current nascent virtual assets ecosystem, new VASPs are in a good position to invest in future trust infrastructures, including infrastructures for attestation verification services. Such services should be part of a broader VASP *managed compliance services* for regulated private wallets. A more in-depth discussion can be found in [37].

REFERENCES

[1] OCC, "Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers (Interpretive Letter 1170)," July 2020. [Online]. Available: https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf

[2] H. Lennon, "Bitcoin Meets Banking As U.S. Bank Regulator Permits Cryptocurrency Custody," *Forbes*, July 2020, https://www.forbes.com/sites/haileylennon/2020/07/22/bitcoin-meets-banking-as-us-bank-regulator-permits-cryptocurrency-custody.

[3] CoinMarketCap.com, "Top Cryptocurrency Spot Exchanges," February 2021, https://coinmarketcap.com/rankings/exchanges/ (Accessed 28 February 2021).

[4] FATF, "International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation," Financial Action Task Force (FATF), FATF Revision of Recommendation 15, October 2018, available at: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

[5] FINMA, "FINMA Guidance: Payments on the blockchain," Swiss Financial Market Supervisory Authority (FINMA), FINMA Guidance Report, August 2019. [Online]. Available: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20190826-finma-aufsichtsmitteilung-02-2019.pdf

[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[7] Ledger, "Ledger Nano X," February 2021. [Online]. Available: https://shop.ledger.com/products/ledger-nano-x

[8] Metaco, "Metaco and Aon announce an insurable crypto asset storage technology for banks," June 2019, https://www.metaco.com/press_releases/metaco-and-aon-announce-an-insurable-crypto-asset-storage-technology-for-banks/.

[9] Trusted Computing Group, "TPM Main – Specification Version 1.2," Trusted Computing Group, TCG Published Specification, October 2003, available at http://www.trustedcomputinggroup.org/ resources/ tpm_main_specification.

[10] ——, "Trusted Platform Module Library Part 1: Architecture – Specification Family 2.0 ," Trusted Computing Group, TCG Published Specification, March 2014. [Online]. Available: https://trustedcomputinggroup.org/wp-content/uploads/TPM-Rev-2.0-Part-1-Architecture-01.07-2014-03-13.pdf

[11] C. Gerber, "Army requires security hardware for all PCs: Coming mandate specifies that new computers contain a standard Trusted Platform Module," *Federal Computer Week*, July 2006. [Online]. Available: https://fcw.com/articles/2006/07/31/army-requires-security-hardware-for-all-pcs.aspx

[12] F. McKeen, I. Alexandrovich, I. Anati, D. Caspi, S. Johnson, R. Leslie-Hurd, and C. Rozas, "Intel Software Guard Extensions (Intel SGX) Support for Dynamic Memory Management Inside an Enclave," in *Proc. Workshop on Hardware and Architectural Support for Security and Privacy (HASP) 2016*, Seoul, June 2016, http://caslab.csl.yale.edu/workshops/hasp2016/program.html.

[13] ARM, "ARM Security Technology: Building a Secure System using TrustZone Technology," ARM Limited, ARM Technical Documentation – PRD29-GENC-009492C, April 2009. [Online]. Available: http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.prd29-genc-009492c/CABGFFIC.html

[14] D. Weston, "Meet the Microsoft Pluton processor - The security chip designed for the future of Windows PCs," November 2020, https://www.microsoft.com/security/blog/2020/11/17/meet-the-microsoft-pluton-processor-the-security-chip-designed-for-the-future-of-windows-pcs.

[15] Microsoft Corp, "Trusted Platform Module and Bitlocker Drive Encryption," https://msdn.microsoft.com/en-us/library/windows/hardware/dn653315.

[16] A. Brandt, "Seagate Maxtor BlackArmor Encrypted Hard Drive," *PC World*, February 2009. [Online]. Available: https://www.pcworld.com/article/158879/seagate_maxtor_blackarmor.html

[17] T. Hardjono and G. Kazmierczak, "Overview of the TPM Key Management Standard," 2008, available on http://www.trustedcomputinggroup.org/ files/ resource_files/.

[18] Trusted Computing Group, "TPM Main – Part 1 Design Principles – Specification Version 1.2," Trusted Computing Group, TCG Published Specification, October 2003, available at http://www.trustedcomputinggroup.org/ resources/ tpm_main_specification.

[19] N. Smith (ed), "TCG Attestation Framework," Trusted Computing Group, TCG Draft Specification – Version 1.0, November 2020.

[20] G. Coker, J. Guttman, P. Loscocco, A. Herzog, J. Millen, B. OHanlon, J. Ramsdell, J. S. Ariel Segall, and B. Sniffen, "Principles of Remote Attestation," *International Journal of Information Security*, vol. 10, pp. 63–81, April 2011. [Online]. Available: https://doi.org/10.1007/s10207-011-0124-7

[21] S. Berger, R. Caceres, K. A. Goldman, R. Perez, R. Sailer, and L. van Doorn, "vTPM: Virtualizing the Trusted Platform Module," in *Security'06: 15th USENIX Security Symposium*, Vancouver, Canada, July-Aug 2006, available on www.usenix.org.

[22] T. Hardjono and N. Smith, "Towards an Attestation Architecture for Blockchain Networks (to appear)," *World Wide Web Journal – Special Issue on Emerging Blockchain Applications and Technology*, 2021. [Online]. Available: https://arxiv.org/abs/2005.04293

[23] I. Allison, "Crypto.com Lands Record $360M Insurance Cover for Offline Bitcoin Vaults," *PC World*, May 2020, https://www.coindesk.com/crypto-com-lands-record-360m-insurance-cover-for-offline-bitcoin-vaults.

[24] A. Walker, "Can Crypto Assets Go Mainstream Without Insurance?" *Insurance Edge*, April 2020. [Online]. Available: https://insurance-edge.net/2020/04/09/can-crypto-assets-go-mainstream-without-insurance/

[25] Bank of England, "Central Bank Digital Currency: Opportunities, challenges and design," Bank of England, Discussion Paper, March 2020, https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper.

[26] ECB, "Report on a Digital Euro," European Central Bank (ECB), Report, October 2020. [Online]. Available: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf

[27] A. Lipton and A. Treccani, *Blockchain and Distributed Ledgers: Mathematics, Technology and Economics*. World Scientific Publishing, Singapore, 2021.

[28] A. Lipton, A. Sardon, F. Schär, and C. Schüpbach, "Stablecoins, Digital Currency, and the Future of Money," April 2020, to appear in *Building the New Economy* (MIT Press 2021).

[29] T. Hardjono, "Blockchain Gateways, Bridges and Delegated Hash-Locks," February 2021. [Online]. Available: https://arxiv.org/abs/2102.03933

[30] T. Hardjono, M. Hargreaves, and N. Smith, "An Interoperability Architecture for Blockchain Gateways," IETF, Internet-Draft draft-hardjono-blockchain-interop-arch-01, October 2020. [Online]. Available: https://datatracker.ietf.org/doc/draft-hardjono-blockchain-interop-arch/

[31] B. Balacheff, L. Chen, S. Pearson, D. Plaquin, and G. Proudler, *Trusted Computing Platforms: TCPA Technology in Context*. New York: Prentice Hall, 2002.

[32] T. Dodson, "Intel Transparent Supply Chain Process," NIST, Winter 2017 Software and Supply Chain Assurance Forum, December 2017. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/ssca/2017-winter/TuePM1_3_%20Intel.pdf

[33] T. Hardjono and N. Smith (ed), "TCG Infrastructure Working Group architecture (Part 2) – Integrity Management – Specification Version 1.0 Rev 1.0," Trusted Computing Group, TCG Published Specification, November 2006, available at http://www.trustedcomputinggroup.org/resources.

[34] Global Semiconductor Alliance, "The GSA Trusted IoT Ecosystem for Security (TIES)," February 2021. [Online]. Available: https://www.gsaglobal.org/wp-content/uploads/2020/09/gsatiesintroduction.pdf

[35] G. Mandyam, L. Lundblade, M. Ballesteros, and J. O'Donoghue, "The Entity Attestation Token (EAT)," IETF, Internet-Draft draft-ietf-rats-eat-03, February 2020. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-rats-eat/

[36] G. Bulk, "How blockchain could transform the world of indirect tax," Ernest Young (EY), Whitepaper, April 2018. [Online]. Available: https://www.ey.com/en_gl/trust/how-blockchain-could-transform-the-world-of-indirect-tax

[37] T. Hardjono, "Attestation Infrastructures for Private Wallets," February 2021. [Online]. Available: https://arxiv.org/abs/2102.12473